

IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): A transmitter device which transmits ~~first data a~~
content to a receiver device by driving a recording medium that stores the ~~first data and~~
~~second data that describes a limitation on the usage of the first data~~ content and management
data changed based on usage of the content, the transmitter device comprising:

storage means for storing a check value calculated on the basis of the ~~second data~~
management data;

communication means which, in authenticating of the receiver device, transmits the
~~second data~~ management data to the receiver device and receives a check value calculated on
the basis of the ~~second data~~ management data and a check value calculated on the basis of
management data changed based on the usage of the content from the receiver device;

determination means ~~which, in the authenticating of the receiver device, determines~~
for determining whether the check value of the ~~second data~~ the management data received by
the communication means matches the check value of the ~~second data~~ management data
stored in the storage means; and

updater means for updating the check value of the management data stored in the
storage means to the check value of the changed management data.

Claim 2 (Currently Amended): A transmitter device according of Claim 1, wherein
the storage means inhibits the writing or reading of the check value of the ~~second data~~
management data in a process other than the authentication process.

Claim 3 (Previously Presented): A transmitter device according to Claim 1, wherein

the storage means is tamper resistant.

Claim 4 (Currently Amended): A ~~transmitting method of a transmitter device which transmits~~ transmitting a content first data to a receiver device by driving a recording medium that stores the content first data and management data changed based on usage of the content second data that describes a limitation on the usage of the first data, the transmitting method comprising:

a step of storing a check value calculated on the basis of the management data second data;

in an authenticating step of the receiver device, a step of communication for transmitting the ~~second~~ management data to the receiver device and for receiving a check value calculated on the basis of the ~~second~~ management data and a check value calculated on the basis of management data changed based on the usage of the content from the receiver device; ~~and~~

in the authenticating of the receiver device, a step of determining whether the check value of the ~~second~~ management data received in the communication step matches the check value of the ~~second~~ management data stored in the storing step; and

a step of updating the check value of the management data stored in the storage means to the check value of the changed management data.

Claim 5 (Currently Amended): A program storage medium for storing a transmission process program for transmitting ~~first data~~ content to a receiver device by driving a recording medium that stores the content first data and ~~second~~ management data changed based on usage of the content that describes a limitation on the usage of the first data, the program executed by a transmitter device and comprising:

a step of storing a check value calculated on the basis of the management data ~~second~~
~~data~~;

in an authenticating step of the receiver device, a step of communication for
transmitting the ~~second~~ management data to the receiver device and for receiving a check
value calculated on the basis of the ~~second~~ management data and a check value calculated on
the basis of management changed data based on the usage of the content from the receiver
device; ~~and~~

in the authenticating of the receiver device, a step of determining whether the check
value of the ~~second~~ management data received in the communication step matches the check
value of the ~~second~~ management data stored in the storing step; ~~and~~

a step of updating the check value of the management data stored in the storage means
to the check value of the changed management data.

Claim 6 (Currently Amended): A receiver device for receiving ~~first data~~ a content
from a transmitter device, the receiver device comprising:

communication means which, in authenticating of the transmitter device, receives
from the transmitter device, ~~second data that describes a limitation on the usage of the first~~
~~data~~ a management data changed based on usage of the content and transmits a check value
calculated on the basis of the ~~second~~ management data to the transmitter device; and

encrypted value generator means for generating the check value of the ~~second~~
management data based on the ~~second~~ management data received by the communication
means, in the authenticating of the transmitter device, said check value for detecting whether
the ~~second~~ management data has been tampered with ~~or not~~.

Claim 7 (Currently Amended): A receiver device according to Claim 6, further comprising

random number generator means for generating a random number having a predetermined bit number, wherein the communication means transmits, to the transmitter device, the check value of the ~~second~~ management data together with the random number generated by the random number generator means.

Claim 8 (Currently Amended): A receiver device according to Claim 6, further comprising ~~usage limiting data generator means which generates, subsequent to the reception of the first data, third data which describes a limitation on the usage of the first data, based on the second data received by the communication means~~ data generator means for generating management data changed based on the usage of the content,

wherein the encrypted value generator means generates a check value generated on the basis of the ~~third data generated by the usage limiting data generator means~~ changed management data, and

the communication means transmits, to the transmitter device, the check value of the management ~~second~~ data together with the check value of the ~~third~~ changed management data.

Claim 9 (Currently Amended): A ~~receiving~~ method of a ~~receiver device~~ for receiving ~~first data~~ content from a transmitter device, comprising:

in the authenticating of the transmitter device, a step of communication for receiving, from the transmitter device, ~~second~~ management data changed based on usage of the content ~~that describes a limitation on the usage of the first data~~ and for transmitting a check value calculated on the basis of the ~~second~~ management data to the transmitter device; and

in the authenticating of the transmitter device, a step of generating a check value of the ~~second~~ management data based on the ~~second~~ management data received in the communication step, said check value for detecting whether said ~~second-value~~ management data has been tampered with ~~or not~~.

Claim 10 (Currently Amended): A program storage medium for storing a reception process program for receiving content ~~first data~~ from a transmitter device, the program executed by a receiver device and comprising:

in the authenticating of the transmitter device, a step of communication for receiving, from the transmitter device, ~~second~~ management data changed based on usage of the content that describes a limitation on the usage of the first data and for transmitting a check value calculated on the basis of the ~~second~~ management data to the transmitter device; and

in the authenticating of the transmitter device, a step of generating a check value of the ~~second~~ management data based on the ~~second~~ management data received in the communication step, said check value for detecting whether said ~~second-value~~ management data has been tampered with ~~or not~~.

Claim 11 (Currently Amended): A communication system comprising a transmitter device which transmits a content ~~first data~~ by driving a recording medium that stores the content ~~first data~~ and ~~second~~ management data changed based on usage of the content that describes a limitation on the usage of the first data, and a receiver device for receiving the content ~~first data~~;

the transmitter device comprising:

storage means for storing a check value calculated on the basis of the ~~second~~ data management data;

first communication means which, in authenticating of the receiver device, transmits the ~~second data~~ management data to the receiver device and receives a check value calculated on the basis of the ~~second data~~ management data and a check value calculated on the basis of management data changed based on the usage of the content from the receiver device; and

determination means ~~which, in the authenticating of the receiver device,~~ determines for determining whether the check value of ~~the second data~~ the management data received by the communication means matches the check value of the ~~second data~~ management data stored in the storage means; and

updater means for updating the check value of the management data stored in the storage means to the check value of the changed management data; and
the receiver device comprising:

second communication means which, in authenticating of the transmitter device, receives from the transmitter device, ~~second data that describes a limitation on the usage of the first data~~ a management data changed based on usage of the content and transmits a check value calculated on the basis of the ~~second~~ management data to the transmitter device; and

encrypted value generator means for generating the check value of the ~~second~~ management data based on the ~~second~~ management data received by the communication means, in the authenticating of the transmitter device, said check value for detecting whether the ~~second~~ management data has been tampered with or not.

Claims 12-25 (Canceled).